AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Maryland

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH TWITTER ID @ASAMAD9134, AS DETAILED IN ATTACHMENT B

Case No. 16-3206-ADC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment B

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, to be reviewed per the protocal in Attachment E

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2339B	providing material support of a terrorist organization
18 U.S.C. § 2339C	unlawful financing of terrorism

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Kyra Dressler, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 9 December 2016

Judge's signature

City and state: Baltimore, Maryland

A. David Copperthite, U.S. Magistrate Judge
Printed name and title

ATTACHMENT B

I. Twitter Account to Be Searched

This warrant applies to information associated with the Twitter profile with username **@asamad9134** that is stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered in San Francisco, California.

II. Information to be disclosed by Twitter

To the extent that the information described in this Attachment is within the possession, custody, or control of Twitter, including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account listed in this Attachment for the period from January 1, 2014 through December 31, 2015:

(a) All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

(b) All past and current usernames, account passwords, and names associated with the account;

(c) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

(d) All IP logs and other documents showing the IP address, date, and time of each login to the account;

(e) All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

(f) All "Tweets" and Direct Messages sent, received, "favorited," or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;

(g) All information from the "Connect" tab for the account, including all lists of Twitter users who have favorited or retweeted Tweets posted by the account, as well as a list of all Tweets that include the username associated with the account (*i.e.*, "mentions" or "replies");

(h) All photographs and images in the user gallery for the account;

(i) All location data associated with the account, including all information collected by the "Tweet With Location" service;

(j) All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;

(k) All data and information that has been deleted by the user;

(l) A list of all of the people that the user follows on Twitter and all people who are following the user (*i.e.*, the user's "following" list and "followers" list);

(m) A list of all users that the account has "unfollowed" or blocked;

(n) All "lists" created by the account;

(o) All information on the "Who to Follow" list for the account;

(p) All privacy and account settings;

(q) All records of Twitter searches performed by the account, including all past searches saved by the account;

(r) All information about connections between the account and third-party websites and applications;

(s) All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

III. Information to be seized by the government

All information described above in Section II that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2339B and 2339C from January 1, 2014, to December 31, 2015, including, for each user ID identified in this Attachment, information pertaining to the following matters:

(a) Records of communication with other individuals concerning the preparation for, planning of, and/or funding of terrorist-related activities;

(b) Information pertaining to the solicitation and/or identification of co-conspirators and/or facilitators involved or associated with Mohammed ELSHINAWY, Tamer EL-KHODARY, ABDUL SAMAD, ATAUL HAQUE, SIFUL SUJAN, ANA GONZALEZ, SHAYMA AKTER, and others involved in undertaking terrorist-related activity in the United States or elsewhere;

(c) Information pertaining to monetary transfers, financial accounts or other monetary instruments that reasonably appear connected to terrorist-related planning or attacks;

(d) Information about the control and operations of IBACS and its related companies, including Ibacstel Electronics, Advance Technology Solutions (also known as Advance Technology Global ("ATG"), and AdvanceTech;

(e) Records indicating that data has been deleted by the account owner, potentially to hide evidence of a crime;

(f) Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

(i) The identity of the person(s) who communicated with the user ID about matters relating to supporting terrorist organizations such as ISIL, including records that might help reveal their whereabouts;

(j) Account history (including Terms of Service and any complaints) and billing records (including date, time, duration, and screen names used each time the account was activated).

ATTACHMENT E

Description of Methods to be Used for Searching Electronically Stored Information

This warrant authorizes the search of electronically stored information. The search shall be conducted pursuant to the following protocol in order to minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search are viewed.

In order to ensure that agents search only those computer accounts and or files described in Section I of Attachments A, B, C and D, this affidavit and the accompanying applications for search warrants seeks authorization to permit employees of the service providers to assist agents in the execution of this warrant. To further ensure that the agents executing the requested warrants search only those computer accounts and/or files described in Section I of Attachments A, B, C and D, the following procedures will be implemented:

a. The search warrant will be presented to the relevant service provider personnel who will be directed to isolate those accounts and files described in Attachments A, B, C and D;

b. In order to minimize any disruption of computer service to innocent third parties, service provider employees (with or without law enforcement personnel) trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Attachments A, B, C and D, including an exact duplicate of all information stored in the computer accounts and files so described;

c. Service provider employees will provide the exact duplicate in electronic form of the accounts and files described in Attachments A, B, C and D, and all information stored in those accounts and files to the agent who serves each warrant;

d. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the service providers' employees and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant, as detailed in Section III of Attachments A, B, C and D; and

e. Law enforcement personnel will then seal the original duplicate of the accounts and files received from service provider employees and will not further review the original duplicate absent an order of the Court.